ANALISIS KEAMANAN WEBSITE DARI SERANGAN SQL INJECTION MENGGUNAKAN WEB APPLICATION FIREWALL

TUGAS AKHIR

Disusun sebagai salah satu syarat untuk kelulusan
Program Strata 1, Program Studi Teknik Informatika,
Universitas Pasundan Bandung

Oleh :

Firdaus Widya Putra
NRP : 11.304.0001

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS PASUNDAN BANDUNG
DESEMBER 2018

LEMBAR PENGESAHAN
LAPORAN TUGAS AKHIR

Telah disetujui dan disahkan Laporan Tugas Akhir, dari :

Nama : Firdaus Widya Putra
Nrp : 11.304.0001

Dengan judul :

"ANALISIS KEAMANAN WEBSITE DARI SERANGAN SQL INJECTION MENGGUNAKAN WEB APPLICATION FIREWALL"

Bandung, 26 Desember 2018

Menyetujui,

Pembimbing Utama,	Pembimbing Pendamping,
(Doddy Ferdiansyah S.T, M.T)	(Ferry Mulyanto, ST., M.Kom)

LEMBAR PENGESAHAN KEASLIAN TUGAS AKHIR

Saya menyatakan dengan sesungguhnya bahwa :

1. Tugas akhir ini adalah benar-benar asli dan belum pernah diajukan untuk mendapatkan gelar akademik, baik di Universitas Pasundan Bandung maupun di Perguruan Tinggi lainnya.
2. Tugas akhir ini merupakan gagasan, rumusan dan penelitian saya sendiri, tanpa bantuan pihak lain kecuali arahan dari tim Dosen Pembimbing.
3. Dalam tugas akhir ini tidak terdapat karya atau pendapat orang lain, kecuali bagian-bagian tertentu dalam penulisan laporan Tugas Akhir yang saya kutip dari hasil karya orang lain telah dituliskan dalam sumbernya secara jelas sesuai dengan norma, kaidah, dan etika penulisan karya ilmiah, serta disebutkan dalam Daftar Pustaka pada tugas akhir ini.
4. Kakas, perangkat lunak, dan alat bantu kerja lainnya yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab saya, bukan tanggung jawab Universitas Pasundan Bandung.

Apabila di kemudian hari ditemukan seluruh atau sebagian Laporan Tugas Akhir ini bukan hasil karya saya sendiri atau adanya plagiasi dalam bagian-bagian tertentu, saya bersedia menerima sangsi akademik, termasuk pencabutan gelar akademik yang saya sandang sesuai dengan norma yang berlaku di Universitas Pasundan, serta perundang-undangan lainnya.

Bandung, 26 Desember 2018

Yang membuat pernyataan,

Materai 6000,-

(Firdaus Widya Putra)

NRP. 11.304.0001

ABSTRAK

Seiring dengan berjalannya waktu, akibat banyaknya para *hacker* muda yang lahir untuk melakukan kejahatan di dunia maya, maka banyak metode yang mereka gunakan untuk melakukan teknik serangan seperti *Cross Site Scripting, Directory Traversal Attack, Parameter Manipulation* dan lain sebagainya. Adapun salah satu contoh teknik serangan yang sering mereka gunakan adalah teknik serangan melalui *SQL injection.*

Setelah mengetahui bahwa SQL *Injection* merupakan suatu teknik serangan *hacker* yang dapat mereka lakukan dari jarak jauh, maka penulis memutuskan untuk mengambil tema ini dengan menggunakan judul ”Analisis Keamanan *Website* dari Serangan *SQL* Injection Menggunakan *Web Application Firewall*”.

Maka berdasarkan dari pengujian teknik SQL *Injection* terhadap website bwapp ini yang telah menggunakan *Mod Security* didapatkan hasil bahwa *SQL Injection* tidak dapat menembus *Website* tersebut.

Kata kunci : Analisis, Kemanan *Website, SQL Injection, WAF, Mod Security*

ABSTRACT

Over time, due to the large number of young hackers born to commit crimes in cyberspace, many methods they use to carry out attack techniques such as Cross Site Scripting, Directory Traversal Attack, Manipulation Parameters and so on. As for one example of the attack technique they often use is attack techniques through SQL injection.

After knowing that SQL Injection is a hacker attack technique that they can do remotely, the author decided to take this theme using the title "Analysis of Website Security from SQL Injection Attacks Using Web Application Firewall".

So based on the testing of SQL Injection techniques on this bwapp website that has used Mod Security, it is found that SQL Injection cannot penetrate the website.

Keyword : *Analysis, Website Security, SQL Injection, WAF, Mod Security*

KATA PENGANTAR

Assalamu'alaikum Wr., Wb.

Puji serta syukur senantiasa penulis panjatkan kahadirat Allah SWT, atas limpahan rahmat serta karunia-Nya penyusun dapat menyelesaikan laporan tugas akhir ini yang merupakan salah satu syarat untuk kelulusan Program Strata 1 di Program Studi Teknik Informatika, Universitas Pasundan Bandung yang berjudul "Analisis Keamanan Website dari Serangan SQL Injection Menggunakan Web Application Firewall" dengan baik.

Dalam penyusunan laporan tugas akhir ini tidak luput dari berbagai kendala, namun berkat bantuan, bimbingan serta kerjasama berbagai pihak sehingga kendala-kendala tersebut dapat diatasi. Dalam kesempatan ini penulis ingin mengucapkan terimakasih yang sebesar-besarnya kepada:

1. Bapak. Dodi Ferdiansyah, S.T, M.T, Ferry Mulyanto, ST., M.Kom selaku pembimbing utama tugas akhir yang selama ini telah membimbing penulis sehingga penulis dapat menyelesaikan tugas akhir.
2. Seluruh civitas akademika Teknik Informatika Universitas Pasundan yang selama ini telah memberikan ilmu kepada penulis.
3. Teman-teman seperjuangan yang tidak bisa penulis sebutkan satu persatu, yang memberikan semangat serta menjadi teman dalam bertukar fikiran.

Dengan segala kerendahan hati, penulis menyadari dalam penyajian laporan tugas akhir ini masih banyak terdapat kekurangan dan jauh dari sempurna, karena kesempurnaan hanyalah milik Allah SWT. Akhir kata penulis mengharapkan kritik dan saran dari pembaca guna perbaikan diwaktu yang akan datang dan semoga Laporan Tugas Akhir ini dapat bermanfaat dan berguna bagi penulis khususnya, juga pihak-pihak lain pada umumnya.

Bandung, 26 Desember 2018

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB 1
PENDAHULUAN

Pada bab ini akan menjelaskan mengenai latar belakang masalah, identifikasi masalah, tujuan tugas akhir, lingkup tugas akhir, metodologi tugas akhir dan sistematika penulisan tugas akhir.

1.1 Latar Belakang Masalah

Kebutuhan dan penggunaan akan teknologi informasi yang diaplikasikan dengan *internet* dalam segala bidang seperti *e-banking*, *ecommerce*, *e-government*, *education* dan banyak lagi telah menjadi sesuatu yang lumrah. Bahkan apabila masyarakat terutama yang hidup di kota besar tidak bersentuhan dengan persoalan teknologi informasi dapat dipandang terbelakang atau ”GAPTEK”.

Internet telah menciptakan dunia baru yang dinamakan *cyberspace* yaitu sebuah dunia komunikasi berbasis komputer yang menawarkan realitas yang baru berbentuk *virtual* (tidak langsung dan tidak nyata). Walaupun dilakukan secara *virtual*, kita dapat merasa seolah-olah ada di tempat tersebut dan melakukan hal-hal yang dilakukan secara nyata, misalnya berkomunikasi, berdiskusi dan banyak lagi.

Perkembangan internet yang semakin hari semakin meningkat baik teknologi dan penggunaannya, membawa banyak dampak baik positif maupun negatif. Tentunya untuk yang bersifat positif kita semua harus mensyukurinya karena banyak manfaat dan kemudahan yang didapat dari teknologi *internet* ini

Kemudian tentunya tidak dapat dipungkiri bahwa teknologi *internet* membawa dampak negatif yang tidak kalah banyak dengan manfaat yang ada. *Internet* membuat kejahatan yang semula bersifat konvensional seperti pengancaman, pencurian dan penipuan kini dapat dilakukan dengan menggunakan media komputer secara *online* dengan risiko tertangkap yang sangat kecil oleh individu maupun kelompok dengan akibat kerugian yang lebih besar baik untuk masyarakat maupun negara disamping menimbulkan kejahatan-kejahatan baru.

Banyaknya dampak negatif yang timbul dan berkembang, membuat suatu paradigma bahwa tidak ada komputer yang aman kecuali dipendam dalam tanah sedalam 100 meter dan tidak memiliki hubungan apapun juga. Ini terbukti dengan banyaknya para *hacker-hacker* pemula yang lahir untuk melakukan tindakan kriminal didunia maya.

Seiring dengan berjalannya waktu, akibat banyaknya para *hacker* muda yang lahir untuk melakukan kejahatan di dunia maya, maka banyak metode yang mereka gunakan untuk melakukan teknik serangan seperti *Cross Site Scripting, Directory Traversal Attack, Parameter Manipulation* dan lain sebagainya. Adapun salah satu contoh teknik serangan yang sering mereka gunakan adalah teknik serangan melalui SQL *injection*.

Sebenarnya SQL *injection* sendiri bukanlah hal baru, dari dulu teknik ini sudah dikenal dalam dunia *hacking* sebagai salah satu teknik *web hacking*, namun baru muncul lagi sekarang karena sifatnya yang dapat merusak *database* dari suatu situs. Teknik yang digunakan dalam SQL *injection* adalah

dengan jalan menginput perintah-perintah standar dalam SQL (DDL, DML, DCL) seperti *create*, *insert*, *upate*, *dorp*, *alter*, *union* dan *select* beserta perintah-perintah lainnya yang tak asing lagi bagi yang sudah mengenal SQL secara mendalam maupun yang baru saja belajar.

SQL singkatan dari *Structured Query Language* yg merupakan bahasa komputer standar yang ditetapkan oleh ANSI (American National Standard Institute) untuk mengakses dan memanupulasi sistem *database*. SQL bekerja dengan program *database* seperti MS Access, DB 2, Informix, MS SQL Server, Oracle, Sybase dan lain sebagainya.

SQL *injection attack* merupakan salah satu teknik dalam melakukan *web hacking* untuk menggapai akses pada sistem *database* yang berbasis SQL. Teknik ini memanfaatkan kelemahan dalam bahasa pemprograman *scripting* pada SQL dalam mengolah suatu sistem *database*. Hasil yg ditimbulkan dari teknik ini membawa masalah yang sangat serius.

Maka setelah mengetahui bahwa SQL *injection* merupakan suatu teknik serangan *hacker* yang dapat mereka lakukan dari jarak jauh, maka penulis memutuskan untuk mengambil tema ini dengan menggunakan judul ”Analisis Keamanan Website dari Serangan SQL Injection Menggunakan Web Application Firewall”.

1.2 Identifikasi Masalah

Adapun masalah yang dapat diidentifikasi yaitu sebagai berikut:

1. Bagaiman cara mengetahui celah dari website bwapp
2. Bagaimana cara meningkatkan Keamanan informasi di dalam website bwapp
3. Bagaimana cara menghasilkan rekomendari dari analisis website bwapp yang dibuat

1.3 Tujuan Tugas Akhir

Adapun tujuan akhir dari tugas akhir kali ini adalah merekomendasikan *tools* yang dapat meminimalisir terjadinya tidakan SQL *Injection* di lingkunan Universitas Pasundan.

1. Mencari celah yang ada di website bwapp
2. Melakukan peningkatan keamanan informasi di website bwapp
3. Menghasilkan rekomendasi dari hasil analisis website bwapp yang telah di kerjakan

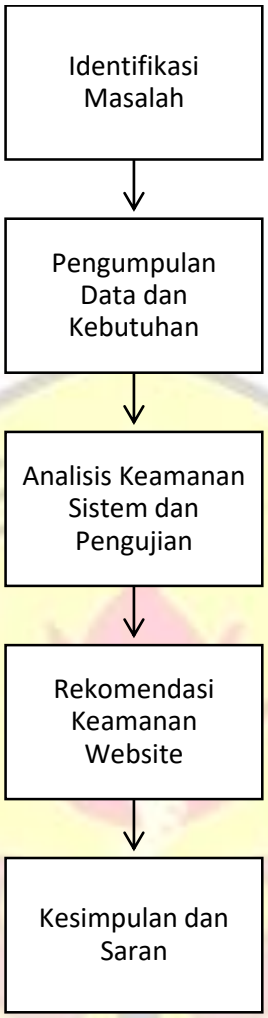
1.4 Lingkup Tugas Akhir

Adapun lingkup dari tugas akhir kali ini adalah

1. Pengujian terhadap Website bwapp.
2. Metode pengamanan menggunakan Mod Security.

1.5 Metodologi Tugas Akhir

Metodologi tugas akhir merupakan gambaran dari langkah-langkah yang dilakukan dalam penyelesaian tugas akhir mengenai perancangan sistem keamanan rumah, sebagaimana ditunjukan pada Gambar 1.1. Metodologi Tugas Akhir.



Gambar 1.1 Metodologi Tugas Akhir

1. Identifikasi Masalah

Tahap awal ini dilakukan untuk mengidentifikasi masalah yang terjadi di lingkungan Universitas Pasundan dan menentukan fokus masalah yang akan di angkat dalam tugas akhir serta menentukan lingkungan implementasi dan pengujian.

2. Pengumpulan Data dan Analisis Kebutuhan

Pengumpulan data dilakukan dengan menggunakan teknik studi literatur. Tahap ini merupakan tahap pengumpulan data yang dibutuhkan dalam pengerjaan tugas akhir. Pengumpulan data dilakukan dengan cara mengumpulkan literatur, jurnal, *paper*, dan artikel-artikel yang terkait dengan judul tugas akhir. Analisis kebutuhan merupakan tahapan analisa terhadap data-data yang sudah dikumpulkan sebagai dasar pelaksanaan tugas akhir.

3. Analisis Keamanan dan Pengujian

Analisis keamanan Website dan penggujiannya dilakukan untuk mengetahui seberapa tinggi keamanan yang ada di dalam website dan seberapa mungkin website itu dapat di *eksploitasi*.

4. Rekomendasi Keamanan Website

Dari hasil analisis dan pengujian yang dilakukan di Bab sebelumnya, maka dihasilkanlah suatu rekomendasi untuk perbaikan website dimasa yang akan data.

5. Kesimpulan dan Saran

Kesimpulan dan saran dihasilkan dari serangkaian aktivitas yang sudah dilaksanakan pada bab-bab sebelumnya.

1.6 Sistematika Penulisan Tugas Akhir

Untuk memudahkan dalam penulisan laporan tugas akhir ini maka diusulkan sistematika penulisan yang mengemukakan mengenai bab-bab pada laporan tugas akhir beserta isinya secara rinci dan keterkaitan dengan bab sebelumnya dan bab setelahnya. Adapun sistematika penulisannya adalah sebagai berikut :

BAB I Pendahuluan

Pada bab ini memberikan penjelasan umum mengenai tugas akhir yang penulis lakukan. Penjelasan tersebut meliputi latar belakang masalah, identifikasi masalah, tujuan tugas akhir, lingkup tugas akhir, batasan masalah, metodologi tugas akhir serta sistematika penulisan.

Bab II Landasan Teori

Pada bab ini memuat teori yang diperlukan untuk pembahasan laporan tugas akhir. Dalam hal ini memuat teori yang berkaitan dengan teori sql *injection*, teori tentang *website* dan juga kerangka kerja yang digunakan.

Bab III Analisis

Pada bab ini membahas mengenai analisis yang sudah dilakukan sebagai landasan dalam penetapan *tools*, lingkungan implementasi dan scenario pengujian yang akan dilakukan.

Bab IV Implementasi dan Pengujian

Pada bab ini menjelaskan mengenai implementasi dan pengujian yang dilakukan pada *web*. Pengujian ini dilakukan untuk mengetahui tolak ukur *web* dalam meminimalisir serangan SQL *Injection*.

Bab V Kesimpulan dan Saran

Pada bab ini menjelaskan tentang kesimpulan dari hasil penelitian dan pembahasan yang telah dipaparkan pada bab sebelumnya serta saran-saran yang diperlukan.

Daftar Pustaka

Bagian ini berisi sumber-sumber yang menjadi acuan penulis dalam mengerjakan tugas akhir.

LAMPIRAN

Berisi penyajian hal-hal yang bersifat khusus sebagai kelengkapan dokumentasi yang perlu dalam penyusunan laporan taugas akhir.

DAFTAR PUSTAKA

[JAM09] Jamiludin, Jaja M, " Best Tools Hacking and Recovery Password", ANDI Offset, 2009.

[MAD15] Made, I Suartana, " Sistem Pengamanan Web Server Dengan Web Application Firewall (WAF)",UPN Veteran Surabaya, Februari 2015.

[RAH13] Rahman, Arief Hakim,"Pendeteksi Serangan SQL Injection Menggunakan Algoritma SQL Injection Free Secure pada Aplikasi Web", Institut Teknologi Sepuluh Nopember, 2013.

[ZUL14] Zulkifli A., Pramana R., Nusyirwan D., "Perancangan Perangkat Pendeteksi Ketinggian Air Bak Pembenihan Ikan Nila Berbasis Mikrokontroler dan Web", Nomor 1, Agustus 2014.

[IDC18] Pengertian Web Server dan Fungsinya, Tersedia : Desember 2018, https://idcloudhost.com/pengertian-web-server-dan-fungsinya/

[IDW18] Pengertian Website Secara Lengkap, Tersedia : Desember 2018, https://idwebhost.com/blog/pengertian-website-secara-lengkap/

[BIN18] Pengertian, Tutorial & Tools SQL Injection, Tersedia : Desember 2018, http://www.binushacker.net/pengertian-tutorial-tools-sql-injection-cara-kumpulan-software-sql-injection.html

[RPS15] Risma Yanti Jamain, Periyadi S.T,M.T., Setia Juli Irzal Ismail, S.T., M.T., "Implementasi Kemanan Aplikasi Web Dengan Web Application Firewall" Fakultas Ilmu Terapan, Universitas Telkom, Desember 2015

[MALM14] Moh Dahlan, ST,.MT, Anastasya Latubessy, S.Kom., M.Cs, Mukhamad Nurkamid, S.Kom., M.Cs, "Pengujian Dan Analisa Kemanan Website Terhadap Serangan SQL Injection", Fakultas Teknik Universitas Muria Kudus, Januari 2014

[KEL95] Kelleher, Kevin, Casey G., Lois D., "Cause and Effect Diagram : Plain & Simple", Joiner Associates Inc, USA, 1995